PCT/IB2004/051840

CLAIMS

1. A method of encrypting data for transmission between first (1) and second (2) communication terminals, the method comprising the steps of:

determining information relating to a time at which a message sent from the first terminal (1) is expected to arrive at the second terminal (2); and

encrypting the data at the first terminal (1) using the determined information.

2. A method according to claim 1, further comprising determining a time of flight for a message sent from one of the first terminal and the second terminal to the other of said terminals.

3. A method according to claim 2, wherein the first and second terminals have first and second internal clocks respectively, each of which generates a sequence of values corresponding to a time sequence, further comprising the step of determining an offset value defining a difference between the sequences of the first and second clocks.

4. A method according to claim 3, wherein the step of determining the estimated time of arrival comprises adding the offset value and the time of flight to a sequence value for the first clock representing the time at which the first message is to be transmitted.

5. A method according to any one of the preceding claims, wherein the step of determining information relating to a time at which the second communication terminal will receive a message sent from the first communication terminal further includes the steps of:

transmitting a first message from the first communication terminal (1) to the second communication terminal (2);

PCT/IB2004/051840

receiving a reply message from the second communication terminal (2), the reply message including information relating to the receipt time of the first message at the second terminal (2) and information relating to a transmission time of the reply message; and

determining the time of receipt of the reply message at the first communication terminal (1).

6. A method according to claim 5, further comprising including the transmission time of the first message with the first message and returning the transmission time of the first message with the reply message.

7. A method according to claim 5, including storing the transmission time of the first message at the first terminal (1) and retrieving the transmission time on receipt of the reply message.

8. A method according to any one of claims 5 to 7, wherein the first and second communication terminals include first and second internal clocks respectively, and the step of determining information relating to the time of receipt comprises determining a value relating to the state of the second internal clock at the time of receipt.

9. A method according to any one of the preceding claims, comprising encrypting the data by combining the determined information with the data.

10. A method according to claim 9, wherein the step of combining the information with the data comprises performing a multiplication operation where a data packet is the multiplicand and the information is the multiplier.

11. A method according to claim 9 or 10, wherein the information comprises a value representing the time at which the message is expected to arrive at the second terminal (2).

PCT/IB2004/051840

12. A method of decrypting encrypted data received from a first communication terminal (1) at a second communication terminal (2), in which the data has been encrypted at the first terminal (1) using information relating to a time at which the data is expected to be received at the second terminal (2), comprising the steps of:

receiving the encrypted data at the second terminal (2);

determining information relating to the time of receipt of the encrypted data; and

using the determined information to decrypt the encrypted data.

13. A method according to claim 12, wherein the first and second terminals (1, 2) include first and second internal clocks (5a, 5b) respectively, and the step of determining information relating to the time of receipt of the encrypted data comprises determining a value relating to the state of the second internal clock (5b) at the time of receipt.

14. A method according to claim 13, wherein the step of using the determined information to decrypt the encrypted data comprises combining the data with the clock related value.

15. A method according to claim 14, wherein the step of combining the data with the clock related value comprises dividing a value representing an encrypted data packet by the clock related value.

16. A method of setting up a secure channel between first and second communication terminals (1, 2) in a communication system, the method comprising the steps of:

receiving a first message sent from the first terminal (1) at the second terminal (2); and

transmitting a second message from the second terminal (2) to the first terminal (1), the second message including information relating to the time of

PCT/IB2004/051840

arrival of the first message at the second terminal (2) and the time of transmission of the second message from the second terminal (2) to the first terminal (1).

17. A method according to claim 16, further comprising the step of determining information relating to the time of transmission of the first message from the first terminal (1).

18. A method according to claim 17, wherein the information relating to the time of transmission is included in the first and second messages.

19. A method according to claim 17, wherein the step of determining information relating to the time of transmission of the first message comprises storing the information at the first terminal (1) on transmission of the first message and retrieving the information from the first terminal (2) on receipt of the second message.

20. A method according to any one of claims 16 to 19, further comprising the step of receiving the second message at the first terminal (1) and determining information relating to the time of receipt of the second message.

21. A communication system in which data is to be encrypted for transmission between first and second communication terminals (1, 2), the system comprising:

means for determining information relating to a time at which a message sent from the first terminal (1) is expected to arrive at the second terminal (2); and

means for encrypting the data at the first terminal (1) using the determined information.

PCT/IB2004/051840

22. A system according to claim 21, wherein the determining means include:

means for transmitting a first message from the first communication terminal (1) to the second communication terminal (2);

means for receiving the first message at the second communication terminal (2) and determining a time of receipt;

means for transmitting a reply message from the second communication terminal (2) to the first communication terminal (1), the reply message including information relating to the receipt time of the first message at the second terminal and information relating to a transmission time of the reply message from the second terminal (2); and

means for receiving the reply message at the first communication terminal (1).

23. A system according to claim 22, wherein the first message transmitting means includes means for including the transmission time of the first message with the first message and the means for transmitting a reply message from the second terminal includes means for including the transmission time of the first message with the reply message.

24. A system according to claim 22, further comprising means for storing the transmission time of the first message at the first terminal (1) and means for retrieving the transmission time of the first message on receipt of the reply message.

25. A system according to any one of claims 21 to 24, wherein the first terminal includes means for transmitting the encrypted data to the second terminal (2).

26. A system according to any one of claims 21 to 25, wherein the first and second terminals have first and second internal clocks (5a, 5b)

PCT/IB2004/051840

respectively, each of which generates a sequence of values corresponding to a time sequence.

27. A system according to claim 26, including means for determining an offset value defining a difference between the sequences of the first and second clocks (5a, 5b).

28. A system according to claim 27, including means for determining a propagation delay between transmission of the message by the first communication terminal (1) and its receipt by the second communication terminal (2).

29. A transmitter (1) configured to transmit encrypted data to a receiver (2), the transmitter (1) comprising:

means for determining information relating to a time at which a message sent from the transmitter (1) is expected to arrive at the receiver (2);

means for encrypting the data at the transmitter (1) using the determined information.

30. A transmitter according to claim 29, further comprising means for including information relating to a transmission time of a message into the message to be transmitted.

31. A transmitter according to claim 29, further comprising means for storing information relating to a transmission time of a message.

32. A transmitter according to claim 31, further comprising means for retrieving the information relating to the transmission time of the message on receipt of the reply message.

33. A receiver (2) configured to decrypt data sent from a transmitter (1), wherein the data is encrypted using information relating to a time at which

PCT/IB2004/051840

a message sent from the transmitter (1) is expected to arrive at the receiver (2), the receiver (2) comprising:

means for receiving the encrypted data;

means for determining a time of arrival of the encrypted data; and

means for decrypting the encrypted data using the determined information.

34. A computer program, which when run on a processor, is configured to carry out the method of any one of claims 1 to 20.